Remarks

Reconsideration is requested in view of the preceding amendments and the following remarks.

The allowance of claims 4, 9-10, 23-24, and 26-28 is acknowledged with gratitude.

Claim 4 was indicated as allowed but depends from rejected claim 29. Therefore, claim 4 is amended to recite the features of claim 29 and claim 5 from which claim 29 depends. Claims 9 and 10 were indicated as allowed but depend from rejected claims 5 and 8, respectively. Claims 9 and 10 are therefore amended to include all the features of their base claims and any intervening claims and are in condition for allowance. Claim 26 was indicated as allowed but depends from rejected claim 5. Therefore, claim 26 is amended to recite the features of claim 5. In view of these amendments, claims 4, 9-10, and 26 remain in condition for allowance.

Claim 19 was indicated as objected to. Claim 17 is amended to recite the features of claim 19, and claim 19 is cancelled. In view of this amendment, claim 17 and dependent claim 18 are properly allowable.

Claim 20 is amended to correct an obvious typographical error.

Claim 5 is also amended. Support for the amendments to claim 5 can be found in the specification at, for example, the paragraph bridging pages 23-24. No new matter is introduced.

Rejections under 35 U.S.C. § 101

Claims 5-8 and 29 stand rejected as being directed to non-statutory subject matter. Claim 5 is amended to clarify that these claims pertain to secure communication of a message from a message sender to a message recipient. In view of the amendment to claim 5, claim 5 and dependent claims 6-8 and 29 are directed to statutory subject matter, and withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 102

Claims 17-18, 20-22, 25, and 30 stand rejected as anticipated by Monier, U.S. Patent 5,745,398 ("Monier"). The rejection of claims 17-18 is moot in view of the amendment of claim 17 to include the features recited in allowable claim 19. Claim 25 depends from allowable claim 17 and is allowable for at least this reason. The rejection of claims 20-22 and 30 is traversed.

The Action states that Monier discloses a plurality of processing elements that includes inputs for words of a multiplicand, words of the modulus, and an output that delivers values of the words of the Montgomery product. Applicants respectfully disagree. While Monier's Fig. 1 circuit receives a multiplier B (input to MUX 13), words A_{i-1} of a multiplicand A (input to MUX 24), and a modulus N (input to MUX 15), Monier's Fig. 1 does not disclose "at least a first processing element and a second processing element, each of the processing elements including inputs that receive words of the first operand and the modulus, and outputs that deliver values of words of the Montgomery product" as recited in claim 20. At most, Monier discloses a single processing element, not first and second processing elements as claimed. In addition, Monier's Fig. 1 circuit receives a modulus N as bits and not words as claimed. Monier's MUX 15 receives the modulus N as a series of bits (not words) and MUX 38 delivers the modulus N as a series of bits (not words). The only portions of Monier's Fig.1 that show paths that can communicate words are the parallel paths associated with the multiplication circuit 19 and registers 16, 21, and the multiplication circuit 20 and registers 17, 18. (Monier shows parallel data paths with wide, hollow arrows, and serial (bit) data paths as lines.)

Claim 21 further recites an input for receiving a value associated with a precision of the first and second operands. In rejecting claim 21, the Action states that Monier recites inputs for receiving words of the multiplicand (first operand), an intermediate value of a word of a Montgomery product,

and an input for a bit of the multiplier (second operand). While Applicants respectfully disagree with this characterization of Monier, the Action does not identify any portion of Monier that corresponds to an input for receiving a value associated with a precision of the first and second operands as recited in claim 21.

Claim 22 further recites that a data path is configured to provide a first selected bit of the second operand to the first processing element, and a second selected bit of the second operand to the second processing element. The Action states that Fig. 1 demonstrates a data path configured to provide a first selected bit of the multiplier (second operand) to the first processing element and a second selected bit of the multiplier (second operand) to a second processing element. Applicant respectfully disagrees. Monier's Fig. 1 shows that bits of the multiplier (B) can only be coupled to the multiplication circuit 19 through subtraction circuit 27 and MUX 25, or through MUX 24, register 16, and flip-flop 21. Thus, bits of the multiplier can be coupled only to a single multiplication circuit 19, and not to first and second processing elements as claimed.

The Action also cites the following portions of Monier:

> Thus, the invention provides a method for the implementation of modular multiplication according to the Montgomery method, wherein a multiplicand A and a multiplier B are encoded respectively on a and b words of k bits, the most significant words of A and B being non-zero, a modulo N is encoded on m words of k bits, the modulo having (m-m') most significant words with k bits at zero, with $0 < m' \leq m$. Col. 3, lines 39-49.

> Thus, it would be possible to carry out operations on operands (i.e. multiplicands and multipliers) of any size. In particular, both these operands could be encoded on a number of words greater than m or greater than the modulo.

> The invention also proposes the following, with B being smaller than or equal to N:
> the producing of $H=2^{(n+m')*k} \bmod N$,

the producing of an intermediate data element encoded on m words of k bits by giving m words, corresponding to B encoded on mn words of k bits, and the a words of A respectively to the serial input and to the parallel input of the multiplication circuit, and

the producing of A*B mod N by giving the m words of the intermediate data element and the m' least significant words of H respectively to the serial input and to the parallel input of the multiplication circuit.

The invention also proposes a method wherein (a+b) and m' are compared, and

If a+b<m', then A*B mod N is produced by giving m words, corresponding to B* 2^{a*k} encoded on m words, and the a words of A respectively to the serial input and to the parallel input of the multiplication circuit.

if a+b=m' then

B*2^{a*k} and N are compared, and

if B*2^{a*k} <N, then A*B mod N is produced by giving m words, corresponding to B *2^{a*k} encoded on m words, and the a words of A respectively to the serial input and to the parallel input of the multiplication circuit.

else A*B mod N is produced by giving m words, corresponding to B*2^{a*k} mod N encoded on m words, and the a words of A respectively to the serial input and to the parallel input of the multiplication circuit. Col. 4, lines 12-45.

None of these portions teaches or suggests first and second processing elements that include inputs that receive words of the first operand and the modulus, and a data path configured to deliver values of words of the Montgomery product from the first processing element to the second processing element as claimed. In addition, no portion of Monier enables any such processing elements, as Monier does not show any word inputs for a modulus or suggest how such word inputs should be situated.

Claim 30 recites a smart card comprising a Montgomery multiplication module having a word input configured to receive words of a modulus and is also allowable over Monier.

In view of the above, independent claims 20 and 30, and dependent claims 21-22 are properly allowable over Monier.

MJ:mj 8/15/05 416422.doc 99-12
PATENT

Attorney Reference Number 245-53434-01
Application Number 09/621,020

Information Disclosure Statement (IDS)

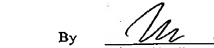
A Supplemental IDS was submitted on November 17, 2004, but an initialed copy of the accompanying PTO FORM 1449 has not been received. Applicants request consideration of the cited reference, and return of the initialed PTO FORM 1449.

Conclusion

In view of the preceding amendments and remarks, all pending claims are in condition for allowance. If any issues remain, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By 

Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 228-9446